



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/646,489	11/02/2000	Edward J. Naclerio	770P009665-U	8816
2512	7590	05/18/2004	EXAMINER	
PERMAN & GREEN 425 POST ROAD FAIRFIELD, CT 06824			WOO, RICHARD SUKYOON	
		ART UNIT	PAPER NUMBER	3629
DATE MAILED: 05/18/2004				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/646,489	NACLERIO
	Examiner	Art Unit
	Richard Woo	3629

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 31 March 2004.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 2 and 4-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 2 and 4-21 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) Notice of Informal Patent Application (PTO-152)
6) Other: _____.

DETAILED ACTION

Response to Arguments

- 1) The Applicant's response filed on March 31, 2004 is acknowledged.
- 2) Applicant's arguments with respect to previous office action have been fully considered and are persuasive. The finality of office action has been withdrawn.
- 3) The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

- 4) Claims 2 and 4-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leon et al. (US 6,591,251) in view of Bergum et al. (US 5,249,227).

W.R.T. Claims 2 and 12:

Leon et al. discloses a method comprising the steps of:

storing the data (encryption key) in a first memory (214) (see col. 4, lines 61-67; col. 5, lines 1-13);

encrypting the body of data with respect to the encryption key (see col. 5, line 51 – col. 7, line 37); and

in the event of tampering with the postal security device, removing power from the memory resulting in a loss of the encryption key (col. 7, lines 6-38).

However, Leon et al. does not specifically disclose the method including:

storing the encrypted body within the first memory;

upon power-up of the PSD decrypting the encrypted body of data with the cryptographic engine;

temporarily storing the decrypted body of data in a third memory, wherein upon power down of the PSD the decrypted body of data is lost; and

in the event of tampering with the PSD, removing power from the second memory and the third memory resulting in a loss of the decrypted body of data.

Bergum et al. teaches, for an encrypted device to improve security, that the device comprises:

a first memory (105); a second memory (106);

a third memory (103) not having a backup battery and storing temporarily the data;

wherein the body of data includes cryptographic keys;

an anti-tamper device to interrupt power to the second memory device and the third memory device (cols. 3-4); and

a detection device adapted to detect the tampering and send a message via a communications channel (113) to an authority, for the purpose of:

storing the data encryption key in a second memory (106);

encrypting the body of data by the cryptographic engine with respect to the encryption key; and

removing power from the second and third memories in the event of tampering with the device.

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the invention of Leon et al. such that the invention includes an improved anti-tamper device to interrupt power to the second memory device and the third memory device, as taught by Bergum et al. for the purpose of preventing an unauthorized user from accessing the PSD (digital encryption/decryption method) and providing a greater security in storing and utilizing encryption/decryption keys when the device loses power, or is tampered with (anti-tampering device).

W.R.T. Claims 13-14: The modified Leon et al. further discloses the method including the step of interrupting power to the second memory device and the third memory device (cols. 3-4 in Bergum et al.);

W.R.T. Claim 15: The modified Leon et al. further discloses the method including the step of minimizing an amount of back-up battery power consumed (Only the second memory has the back-up battery, no battery for the first and third memories);

W.R.T. Claim 16: The modified Leon et al. further discloses the method including the step of storing only the encryption key and the encrypted body of data when no power is supplied to the postal security device and only the back-up power is supplied to the second memory (see Supra Bergum et al. and Leon et al. for the memory arrangements);

W.R.T. Claim 17: The modified Leon et al. further discloses the method including the step of generating a postal indicia and printing the indicia based on the data (see the postage meter of Leon et al.);

W.R.T. Claim 18: The modified Leon et al. further discloses the method including the step of, upon power-up of the PSD, detecting a presence of the encryption key, and if not present, transmitting a message to an administrator of the PSD indicating a breach of the PSD (see Supra Bergum et al.);

W.R.T. Claim 19: The modified Leon et al. further discloses the method including the step of maximizing a life of the battery powering the second memory by limiting a size of data stored in the second memory to the encryption key (obviously smaller the size of data stored, smaller the power consumption of the batter);

W.R.T. Claim 20: The modified Leon et al. further discloses the method including the step of minimizing the need for back-up battery power in the PSD (see Supra Claim 15);

W.R.T. Claim 21: The modified Leon et al. further discloses the method including the step of determining that the data in the second memory is lost and automatically notifying the authority (obvious to notify the authority upon the detection of tampering).

W.R.T. Claims 4 and 9:

Leon et al. further discloses a postal security device comprising:

a secure housing;

an encryption engine adapted to encrypt the body of data with respect to the encryption key; and

a first nonvolatile memory (214; col. 4, lines 61-67) storing encryption keys.

However, Leon et al. does not specifically disclose the device including:
the second NVM having a storage capacity only large enough to store an
encryption key;
the third memory device temporarily storing a body of decrypted data while PSD
is powered on, wherein upon power down of the PSD the decrypted body of data is lost;
and
wherein the PSD powers down or the power is interrupted, the body of decrypted
data temporarily stored in the third memory is lost.

Bergum et al. teaches, for an encrypted device to improve security, that the
device comprises:

a first memory (105); a second memory (106);
a third memory (103) not having a backup battery and storing temporarily the
data;
wherein the body of data includes cryptographic keys;
an anti-tamper device to interrupt power to the second memory device and the
third memory device (cols. 3-4); and
a detection device adapted to detect the tempering and send a message via a
communications channel (113) to an authority, for the purpose of:
storing the data encryption key in a second memory (106);

encrypting the body of data by the cryptographic engine with respect to the encryption key; and

removing power from the second and third memories in the event of tampering with the device.

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the invention of Leon et al. such that the invention includes an improved anti-tamper device to interrupt power to the second memory device and the third memory device, as taught by Bergum et al. for the purpose of preventing an unauthorized user from accessing the PSD (digital encryption/decryption method) and providing a greater security in storing and utilizing encryption/decryption keys when the device loses power, or is tampered with (anti-tampering device). Additionally, it would have been obvious at the time the time the invention was made to a person having ordinary skill in the art to make the second NVM having a storage capacity only large enough to store an encryption key as an engineering expedient for the purpose of providing the PSD with a cost-effective memory device (a bigger memory device usually means more expensive) and the improved battery life (a memory with smaller size consumes less power).

W.R.T. Claims 5 and 11: The modified Leon et al. further discloses device including a means for generating a postal indicia and printing the indicia based on the data (see postage meter in Leon et al.);

W.R.T. Claims 6 and 10: The modified Leon et al. further discloses device including an anti-tamper device to interrupt power to the second memory device and the third memory device (see the anti-tamper device in Leon et al. and cols. 3-4 in Bergum et al.);

W.R.T. Claim 7: The modified Leon et al. further discloses device wherein the body of data includes cryptographic keys and sensitive bit-images (see Supra Leon et al.); and

W.R.T. Claim 8: The modified Leon et al. further discloses device including a means for transmitting a message (via communication link in Leon et al.) to an authority when the PSD is tampered with.

Conclusion

5) Any inquiry concerning this communication or earlier communications from the examiner should be directed to Richard Woo whose telephone number is 703-308-7830. The examiner can normally be reached on Monday-Friday from 8:30 AM -5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Weiss can be reached on 703-308-2702. The fax phone numbers for the organization where this application or proceeding is assigned are 703-872-9306 for regular communications and for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-0861.


Richard Woo
Patent Examiner
GAU 3629
May 17, 2004

JOHN G. WEISS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600